IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

MICROSOFT CORPORATION, a Washington corporation, Plaintiff, v. JOHN DOES 1-2 CONTROLLING A COMPUTER NETWORK THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS, Defendants.	)	Civil Action No: 1:21-cv-822

COMPLAINT

This is an action to disrupt the technical malicious infrastructure of a sophisticated online criminal network that is attacking Microsoft Corporation ("Microsoft"), its Office 365 ("O365") service, and its customers through malicious "homoglyph" domains that unlawfully impersonate legitimate Microsoft O365 customers and their businesses. Homoglyph attacks rely on elaborate deception that leverages the similarities of character scripts to create imposter domains used to deceive unsuspecting individuals. Defendants use malicious homoglyph domains together with stolen customer credentials to unlawfully access customer accounts, monitor customer email traffic, gather intelligence on pending financial transactions, and criminally impersonate O365 customers, all in an attempt to deceive their victims into transferring funds to the cybercriminals. The relief sought in this action is necessary to stop the cybercriminals and prevent irreparable and ongoing harm to Microsoft and its customers.

Microsoft hereby complains and alleges that John Does 1-2 (collectively "Defendants") target Microsoft's O365 customers and services and conduct malicious activity

including business email compromise attacks ("BEC"), using the Internet domains set forth at **Appendix A** to this Complaint which are referred to as the "Malicious Infrastructure."

NATURE OF THE ACTION

1. This is an action based upon: (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030), (2) the Stored Communications Act (18 U.S.C. § 2701 *et seq.*), (3) the Virginia Computer Crimes Act (Virginia Code Ann. § 18.2-152.5:1), and (4) the common law of trespass to chattels and conversion. Plaintiff seeks injunctive and other equitable relief and damages against Defendants who, through their illegal activities, have caused and continue to cause irreparable injury to Microsoft, its customers, and the public.

PARTIES

2. Plaintiff Microsoft is a corporation duly organized and existing under the laws of the State of Washington, having its headquarters and principal place of business in Redmond, Washington.

3. On information and belief, John Doe 1 deployed and controls the Malicious Infrastructure in furtherance of conduct designed to cause harm to Microsoft, its customers, and the public. Microsoft is informed and believes and thereupon alleges that John Doe 1 can likely be contacted directly or through third-parties using the information set forth in **Appendix A**.

4. On information and belief, John Doe 2 deployed and controls the Malicious Infrastructure in furtherance of conduct designed to cause harm to Microsoft, its customers, and the public. Microsoft is informed and believes and thereupon alleges that John Doe 2 can likely be contacted directly or through third-parties using the information set forth in **Appendix A**.

5. Third party NameSilo LLC is the domain registrar affiliated with the domain names ending in ".com" and ".co," used by Defendants. NameSilo is located at 8825 N. 23rd

Avenue, Suite 100, Phoenix, AZ 85021, United States.

6. Third party Key-Systems GmbH C is the domain registrar affiliated with the domain names ending in ".ca," used by Defendants. Key-Systems is located at Im Oberen Werk 1, 66386 St. Ingbert, Germany.

7. The Defendants have utilized the domain registration facilities of third party domain registry Verisign, Inc., Verisign Information Services, Inc., and Verisign Global Registry Services (collectively, "Verisign") which are the domain name registry entities that oversee the registration of all domain names ending in ".com," including the domains used by Defendants. Verisign is located in the Eastern District of Virginia at 12061 Bluemont Way, Reston, Virginia 20190, United States.

8. On information and belief, Defendants jointly own, rent, lease, or otherwise have dominion over and access to the Malicious Infrastructure used to carry out the cyberattacks that are the subject of this complaint. Microsoft will amend this complaint to allege Defendants' true names and capacities when ascertained. Microsoft will exercise due diligence to determine Defendants' true names, capacities, and contact information, and to effect service upon those Defendants.

9. Microsoft is informed and believes and thereupon alleges that each of the fictitiously named Defendants is responsible in some manner for the occurrences herein alleged, and that Microsoft's injuries as herein alleged were proximately caused by such Defendants.

10. On information and belief, the actions and omissions alleged herein to have been undertaken by Defendants were actions that they, and each of them, authorized, controlled, directed, or had the ability to authorize, control or direct, and/or were actions and omissions each Defendant assisted, participated in, or otherwise encouraged, and are actions for which each

Defendant is liable. Each Defendant aided and abetted the actions and omissions of Defendants set forth below, in that each Defendant had knowledge of those actions and omissions, provided assistance, and benefited from those actions and omissions, in whole or in part. Each Defendant was the agent of each of the remaining Defendants, and in doing the things hereinafter alleged, was acting within the course and scope of such agency and with the permission and consent of other Defendants.

JURISDICTION AND VENUE

11. The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because this action arises out of Defendants' violation of the Computer Fraud and Abuse Act (18 U.S.C. § 1030) and the Stored Communications Act (18 U.S.C. § 2701 *et seq.*). The Court also has subject matter jurisdiction over Microsoft's claims for trespass to chattels, conversion, and the Virginia Computer Crimes Act (Virginia Code Ann. § 18.2-152.5:1) pursuant to 28 U.S.C. § 1367.

12. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to Microsoft's claims has occurred in this judicial district, because a substantial part of the property that is the subject of Microsoft's claims is situated in this judicial district, and because a substantial part of the harm caused by Defendants has occurred in this judicial district. Defendants maintain Internet domains registered in Virginia, engage in other conduct availing themselves of the privilege of conducting business in Virginia, and utilize instrumentalities located in Virginia and the Eastern District of Virginia to carry out acts alleged herein. Venue is proper in this judicial district under 28 U.S.C. § 1391(c) because Defendants are subject to personal jurisdiction in this judicial district.

13. Defendants' Malicious Infrastructure, particularly domain names, is registered

through Verisign, which resides in the Eastern District of Virginia. Defendants use these domains to target Microsoft and its customers. Defendants have undertaken the acts alleged herein with knowledge that such acts would cause harm through domains located in and maintained through facilities in the Eastern District of Virginia, targeting Microsoft's customers and their networks in the Eastern District of Virginia and elsewhere in the United States, thereby injury Microsoft and its customers. Therefore, this Court has personal jurisdiction over Defendants.

FACTUAL BACKGROUND

Microsoft's Services and Reputation

14. Microsoft® is a provider of the Office 365® cloud-based business and productivity suite of services. Microsoft has invested substantial resources in developing high-quality products and services. Due to the high quality and effectiveness of Microsoft's products and services and the expenditure of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, established a strong brand, and developed the Microsoft name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade.

Overview of Defendants' Scheme

15. Sophisticated cybercriminals have engaged in a complex scheme to target Microsoft's O365 customers and services and conduct malicious activity including business email compromise attacks, using stolen credentials to access O365 customer email accounts, imitate customer employees, and target their trusted networks, vendors, contractors, and agents in an effort to deceive them into sending or approving fraudulent financial payments.

16. Defendants' attack typically unfolds as follows:

17. In the first phase, Doe Defendants use stolen O365 login credentials, typically

obtained through deceptive efforts like credential phishing emails which enables unauthorized access to Microsoft's customers' O365 accounts.

18. In the second phase, after using stolen customer credentials to gain unauthorized access to the compromised Office 365 account, Defendants begin reconnaissance, which includes monitoring the compromised account, emails, and contact list to identify opportunities to target the compromised O365 customer's contacts for financial fraud, which may include forwarding emails with key financial words like "invoice," "accounts receivable," "funds," "overdue," "payroll," or "IBAN," and masking their activities to evade detection.

19. In the final phase, having used stolen credentials to gain unauthorized access to Office 365 accounts and having monitored account activity, Defendants identify additional victims either in the compromised O365 customer's business or their wider network (typically, customers, vendors, or agents), who routinely deal with wire transfer requests, invoices, or billing statements and could be deceived by fraudulent requests for payment imitating legitimate payment communications. In this final phase, Defendants register homoglyph domains to impersonate legitimate businesses (hereinafter, "homoglyph imposter domains"), host these homoglyph imposter domains on a fraudulently procured O365 tenant, establish spoof email addresses impersonating one or more of the foregoing parties, all of which is designed to enable Defendants to deceive such parties into sending wire payments to Defendants. In all cases, the Defendants use fraudulent information in an attempt to direct funds to themselves.

Overview of Defendants

20. The precise identities and locations of the cybercriminals behind this unlawful scheme are generally unknown, but they targeted Microsoft customers and their networks across the globe including those located in Virginia and did so by registering homoglyph imposter

domains through domain registries located in the Eastern District of Virginia.

21. Defendants registered Internet domains using means that obfuscate their identities. In some cases, Defendants registered domains through private registration services, which conceal the contact information ordinarily available in the WHOIS database. In other cases, Defendants registered domains using free e-mail addresses that do not provide any indication of the registrants' identities. To the extent that other contact information is visible, Microsoft has not been able to associate such information to any real individual. On some occasions, for the private registration services, where WHOIS information is ordinarily concealed, Defendants are sometimes assigned arbitrary "proxy" email addresses associated with domain names and make those email addresses available in the public WHOIS database. The private registration services provide the proxy email addresses publicly for the purpose of enabling communication with Defendants regarding their domain names. Thus, for each domain, there is an email address that serves as a known point of contact with the Defendants. Email addresses are the only known possible way of communicating the existence of this action specifically to the Defendants.

Overview of Microsoft's Efforts to Protect Customers and Defendants' Attempts to Evade Such Efforts

22. Microsoft commits tremendous resources to protect its online services and works with customers to detect and prevent threats their accounts and data. Microsoft recently detected evidence of Defendants' malicious activity and promptly began to identify patterns and attempted to block Defendants' activity through the technical tools at its disposal. Defendants' activities victimize Microsoft's customers in two ways – first, they use stolen credentials to gain unauthorized access to and compromise accounts of O365 customers ("compromised account victim"), and second, they use this unauthorized access to O365 accounts to exfiltrate

information and develop intelligence about financial transactions from the compromised account victim's wider network – including customers, vendors, or agents ("financial fraud victims") whether they are other O365 users or users of other email platforms. Defendants frequently target senior managers, financial roles (accountants, bookkeepers, etc.), and sales positions (purchasing and services) in a variety of industries.

23. Further, to the extent Defendants have registered homoglyph imposter domains and are hosting those homoglyph imposter domains on O365 tenants that Defendants have fraudulently set up to carry out their criminal schemes, Microsoft takes steps to identify and block the ability of Defendants to use such fraudulent tenants and related accounts for malicious purposes.

24. Yet, even with such self-help measures, the risk of irreparable harm still exists because, even after Microsoft prevents and disables use of O365 for this fraud, Defendants are nonetheless able to move these homoglyph imposter domains to other third-party domain registrars and hosting facilities outside the Microsoft ecosystem. In this way, Defendants are then able to continue criminal activities directed at Microsoft and O365 customers. It is also possible that Defendants register domains and host them from inception outside of Microsoft's ecosystem, placing them beyond Microsoft's internal mitigation measures. In all such scenarios, by maintaining access and control of these homoglyph imposter domains through third-party domain registrars and hosting companies, Defendants continue to target Microsoft's customers and others for financial fraud and other cybercrime.

25. There is a substantial risk from this situation that, notwithstanding Microsoft's significant steps to disable and block malicious infrastructure, Microsoft's customers may incorrectly blame Microsoft for Defendants' continued ability to use homoglyph imposter

domains to target them for fraud and may incorrectly associate Microsoft with the harm caused by Defendants.

26. Defendants' ability to mobilize and move malicious domains presents an ongoing threat to Microsoft's customers and others and undermines Microsoft's efforts to protect its customers and networks. Without the relief requested from this Court, Microsoft will be engaged in a constant game of whack-a-mole where it attempts to protect its customers by shutting down Defendants' malicious activity using tools at its disposal within O365, only to have Defendants move their malicious domains to another domain registrar or hosting company, where the domain can be administered and email services set up by Defendants on other companies' email services, thus enabling Defendants to continue their attacks against Microsoft and Microsoft customers and their networks. This risk is not theoretical, as there is already evidence that Defendants have moved one of the domains from the O365 environment to another hosting company and thereby taken it outside Microsoft's reach.

27. Defendants continue to evolve their tactics in an attempt to avoid detection by Microsoft's customers and to evade Microsoft's numerous safeguards. Given the risk posed by Defendants reconstituting and moving their operations to commit further malicious acts, Defendants pose a current and ongoing threat to Microsoft and the security of its customers such that it is necessary to seek immediate relief in this action.

Microsoft's Office 365 Services and Protection Measures

28. Office 365 is an online service that provides, among other things, access to Microsoft's Office software on a subscription basis. Customers purchase a subscription to Office 365 that may provide access to both cloud and locally stored versions of the software. Use of Office 365 requires an online account.

29. Microsoft goes to great lengths to protect customer accounts. In particular, Microsoft engineered Office 365 with the intent to eliminate threats before reaching Office 365 users. Microsoft uses real-time anti-spam and multiple anti-malware engines to prevent threats from reaching their inboxes. Microsoft also offers Microsoft Defender for Office 365,[1] which helps protect customers against new, sophisticated attacks in real time. In addition to incorporating tools to stop phishing emails before they reach users, Microsoft also investigates the underlying phishing attacks to identify and prevent malicious attacks carried out by criminal organizations.

Defendants Use Unauthorized Access to Microsoft Office 365 Customers' Accounts to Target Their Businesses and Larger Networks

30. Through various investigative techniques, Microsoft recently uncovered Defendants' scheme to gain unauthorized access and compromise O365 accounts, create homoglyph imposter domains, and use this malicious infrastructure and surveillance efforts to target compromised account victim's wider network – including customers, vendors, or agents – for fraudulent financial transactions.

Phase One: Unauthorized Access to Office 365 Using Stolen Credentials

31. The first phase of the business email compromise scheme involves stealing Microsoft O365 credentials through among other means sending credential phishing emails and using malicious websites to socially engineer victims into divulging their account login credentials.

32. Credentials are most typically stolen through an attacker sending a "phishing" email to the victim that contains a link to a malicious website used to socially engineer victims

[1] *See generally* https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-advanced-threat-protection-service-description.

into divulging their account login credentials. Attackers accomplish this by using email domains chosen to impersonate trusted domains or appear otherwise legitimate, and malicious websites set up to impersonate legitimate Microsoft login pages (*e.g.,* using trademark/copyright infringing images to spoof a legitimate Microsoft landing page). The attackers' goal is to deceive targeted victims such that they visit the malicious site and enter their Office 365 account credentials into a counterfeit login page, and those credentials are then captured for subsequent use by an attacker. These types of malicious attacks persist despite the fact that Microsoft encourages all its customers to use certain precautions to protect account credentials such as enabling two factor authentication. Regardless of the method of compromise, Defendants' subsequent use of the stolen credentials to unlawfully access accounts can be identified and observed.

33. Defendants, who make unauthorized access to Office 365 accounts, may engage in the initial phishing activities to obtain credentials to access those accounts or they may acquire such stolen credentials from other cybercriminals. At this juncture, Microsoft does not know which approach Defendants have taken. Nonetheless, Defendants ultimately have in their possession stolen Office 365 credentials which are used for malicious purposes described herein. Regardless of whether Defendants engaged in the initial theft of the credentials or purchased stolen credentials, Defendants are using such credentials to cause severe harm to Microsoft and its customers.

Phase Two: Monitoring Compromised Office 365 Account Email Traffic and Contacts to Identify Opportunities for Further Criminal Activities

34. In the second phase, once Defendants unlawfully gain access to an Office 365 account using stolen credentials, they begin reconnaissance of the compromised account and the compromised account victim's networks in a few ways. Defendants go through the

compromised account victim's Office 365 email mailboxes, stored contacts, and address books to identify opportunities to target customers, vendors, and agents within the compromised account owner's network to solicit fraudulent financial transactions.

35. Defendants either directly monitor the contents of the mailbox or engage in "forwarding" of emails in the compromised email account in order to identify and review communications regarding financial transactions. For example, Defendants access or forward emails containing keywords such as "invoice," "accounts receivable," "funds," "overdue," "payroll," or "IBAN." Defendants either directly access or forward emails with keywords to a collection email account controlled and monitored by Defendants for further analysis. In an effort to avoid detection, Defendants may use unauthorized access to the account to mark any alerts or warnings about their activity as "read," hiding their changes to the account to avoid detection and alerting the owner of the compromised O365 account.

36. Defendants identify key emails and senders to impersonate and identify recipients to target. Defendants then register homoglyph imposter domains and spoof email addresses on those domains. Defendants use these homoglyph imposter domains and email addresses to fraudulently insert themselves into ongoing business transactions or socially engineer opportunities to interact with the financial or billing department of victims. Defendants take advantage of the fact that these emails are designed to appear legitimate and imitate legitimate email addresses that are trusted or known contacts of the recipient, and are part of existing, legitimate communications.

37. Once they have used stolen credentials to access O365 accounts, Defendants are opportunistic in identifying potential financial fraud victims – anyone who might be mentioned in emails, contact lists, or other communications in the compromised account users' account –

and often widen the pool of their victims beyond O365 to other email platforms outside of Microsoft's control.

Phase Three: Impersonating O365 Account Owners or Members of Their Networks to Solicit Fraudulent Financial Transactions

38. In the final phase, having analyzed e-mail traffic from multiple endpoints and monitored for upcoming financial transactions, invoices, bank payment information, or payment details, Defendants set up homoglyph imposter domains together with spoofed email addresses to impersonate O365 account owners or members of their networks and solicit fraudulent financial transactions.

39. Defendants use unlawful access to the compromised O365 account and its content to build out the necessary malicious infrastructure to launch attacks including registering one or more homoglyph imposter domains and creating email addresses that impersonate real people identified during the reconnaissance phase.

40. Defendants create malicious domains that are "homoglyphs" of legitimate domain names. Homoglyphs are a technique by which attackers abuse similarities of character scripts to create deceptively similar domains. For example, a homoglyph domain may utilize characters with shapes that appear identical or very similar to the characters of a legitimate domain. Defendants' efforts to imitate legitimate domains using fraudulent homoglyph variants are clear from the examples below:

- **Defendants add a single letter**:

Legitimate	Impersonation
junctionfueling.com	junctionfuelings.com (Adds an "s")

- **Defendants replace letters with similar appearing letters**:

Legitimate	Impersonation
leaseaccelerator.com	leaseacceierator.com (Changes "l" to "i")

lithiumamericas.com	lithlumamericas.com (Changes “i” to “l”)
sliao.ca	sllao.ca (Changes “i” to “l”)

- **Defendants change top level domain information**:

Legitimate	Impersonation
ccp.edu	ccp-edu.com (Adds .com)

41. Once Defendants’ homoglyph imposter domains are registered and operational, they can send spoofed emails from these homoglyph imposter domains which impersonate the compromised account victim or other legitimate contacts of the target – who might typically respond to requests to pay wire transfer requests, invoices, or billing statements.

42. Defendants, leveraging unauthorized access to the O365 account, can copy the entire body of a prior legitimate email chain, use identical names and signature blocks, but send the impersonation email from a spoofed email address from a homoglyph mail exchange domain which impersonates a legitimate Microsoft O365 customer.

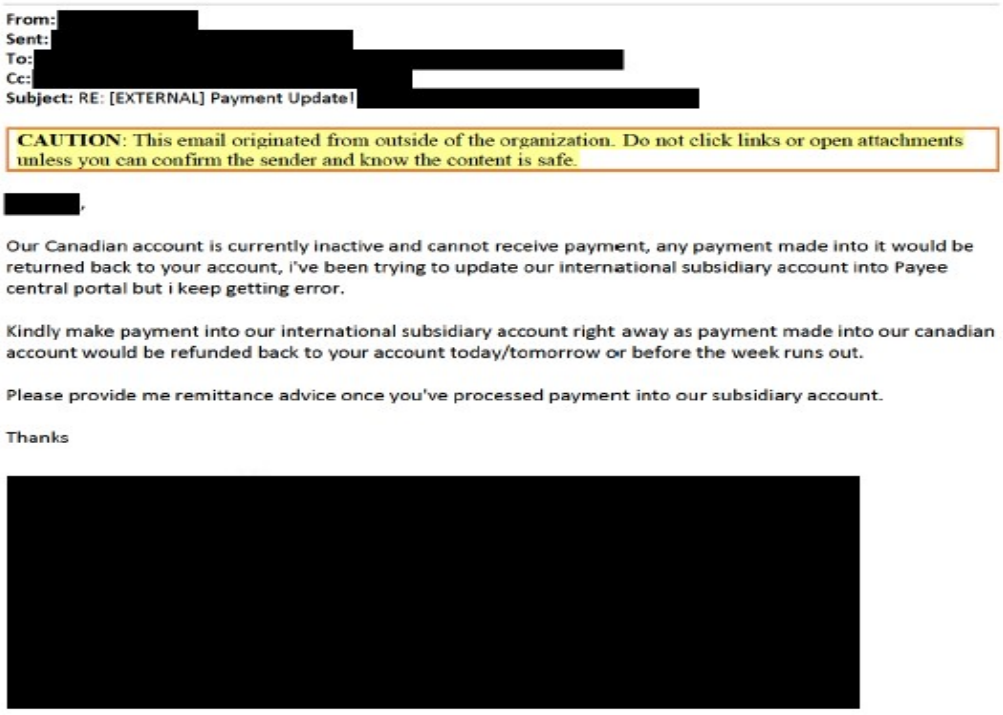
43. Defendants’ fraudulent email communications build on existing, legitimate email communications, course of dealings, or business relationships. Defendants have access to prior email chains, can familiarize themselves with key terminology or terms of art, relevant documents, invoices, or account numbers. Defendants have unauthorized access to information that enables them to leverage existing conversations to try to convince victims to reveal critical business or financial information or process or redirect a payment request or invoice. Defendants commonly use an excuse about why new financial transfer information is being provided or threaten the victim for failure to provide payment or other strategies to create urgency and justify new payment arrangements. These strategies often include providing doctored invoice documents and tampered banking information. The financial fraud victims have no reason to suspect anything malicious, as the email appears to be from a known, legitimate email address,

references existing conversations or prior communications, and provides doctored imitations of real financial documents.

44. In all cases, the Defendants use fraudulent information to unlawfully direct funds to themselves.

45. One example of a business compromise email sent in this case is included below and demonstrates how it mirrors genuine email traffic and instructs the financial fraud victim to redirect an invoice payment.

46. Defendants identified a legitimate email communication from the compromised account of an Office 365 customer referencing payment issues and asking for advice on processing payment:



From: [redacted]
Sent: [redacted]
To: [redacted]
Cc: [redacted]
Subject: RE: [EXTERNAL] Payment Update!

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you can confirm the sender and know the content is safe.

[redacted],

Our Canadian account is currently inactive and cannot receive payment, any payment made into it would be returned back to your account, i've been trying to update our international subsidiary account into Payee central portal but i keep getting error.

Kindly make payment into our international subsidiary account right away as payment made into our canadian account would be refunded back to your account today/tomorrow or before the week runs out.

Please provide me remittance advice once you've processed payment into our subsidiary account.

Thanks

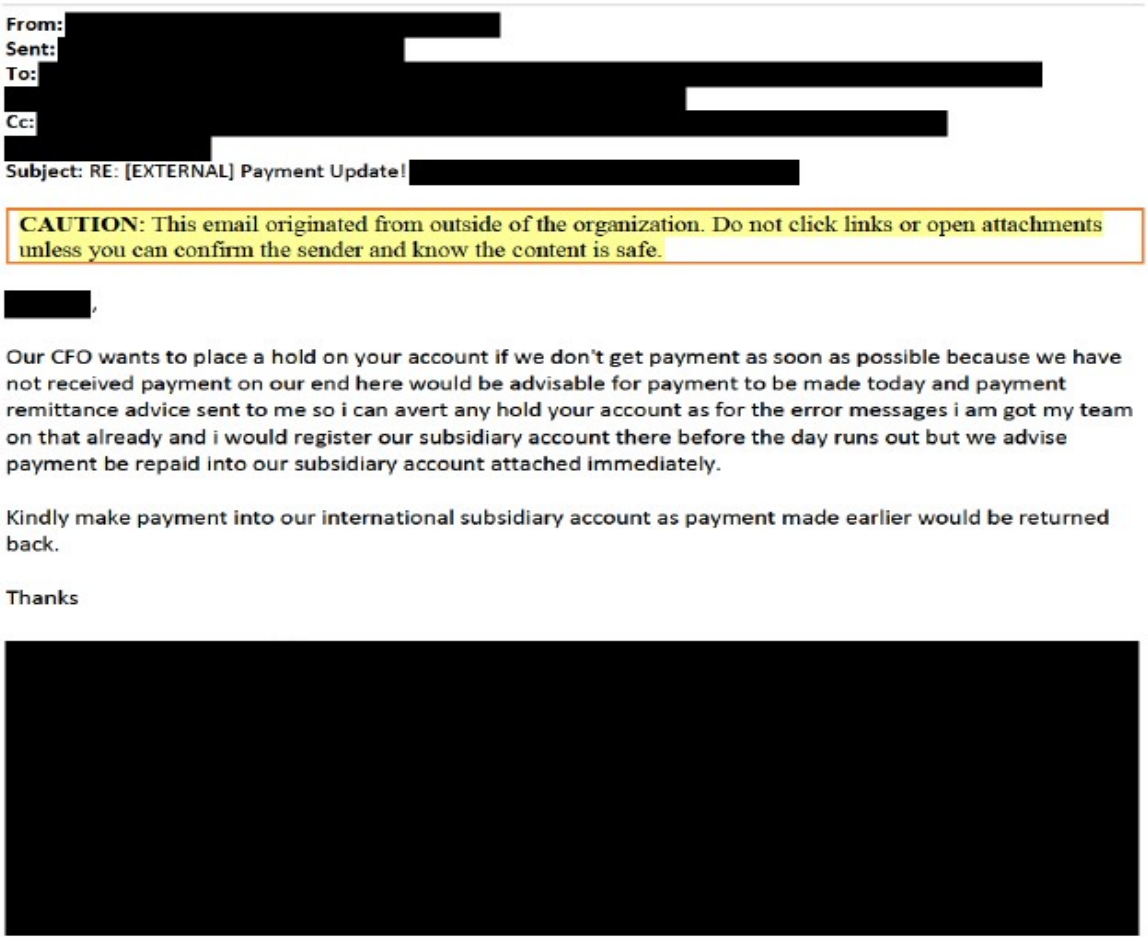
[redacted]

Figure 1

47. Defendants capitalized on this opportunity and sent an impersonation email from a homoglyph imposter domain using the *same sender name* and *nearly identical domain*. The

only difference between the genuine communication and the imposter communication was a single letter changed in the mail exchange domain – changing sliao.ca to sllao.ca – done to escape notice of the recipient and deceive them into believing the email was a legitimate communication from a known trusted source.

48. Defendants used the same subject line and format of an email from the earlier, legitimate conversation, but falsely claimed a hold was placed on the account by the CFO, time was running out, and payment needed to be received as soon as possible:



From: [redacted]
Sent: [redacted]
To: [redacted]
Cc: [redacted]
Subject: RE: [EXTERNAL] Payment Update! [redacted]

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you can confirm the sender and know the content is safe.

[redacted],

Our CFO wants to place a hold on your account if we don't get payment as soon as possible because we have not received payment on our end here would be advisable for payment to be made today and payment remittance advice sent to me so i can avert any hold your account as for the error messages i am got my team on that already and i would register our subsidiary account there before the day runs out but we advise payment be repaid into our subsidiary account attached immediately.

Kindly make payment into our international subsidiary account as payment made earlier would be returned back.

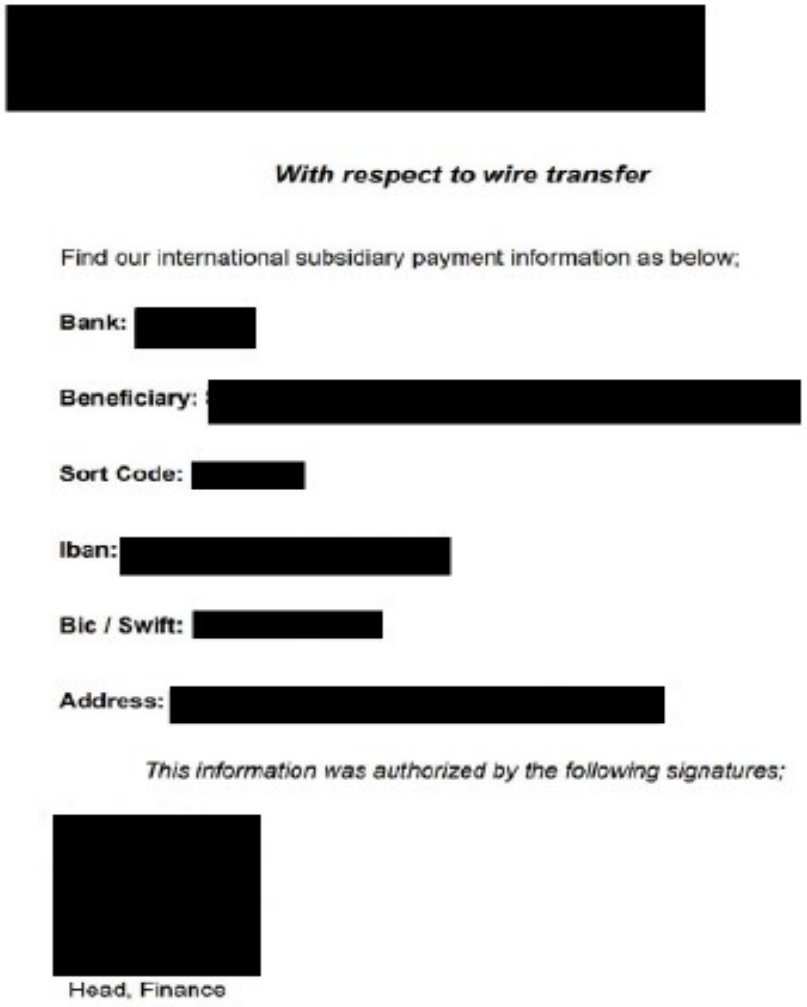
Thanks

[redacted]

Figure 2

49. Defendants then solicit a fraudulent wire transfer by sending new wire transfer information appearing to be legitimate and including company logo information, requesting

funds be sent to Defendants:


[redacted]

With respect to wire transfer

Find our international subsidiary payment information as below;

Bank: [redacted]

Beneficiary: [redacted]

Sort Code: [redacted]

Iban: [redacted]

Bic / Swift: [redacted]

Address: [redacted]

This information was authorized by the following signatures;

[redacted]

Head, Finance

50. Defendants do not rely on malicious links or attachments in these communications – instead using the intelligence needed to imitate legitimate business transactions gathered after unlawfully accessing a compromised account– in an effort to evade detection and which makes it more difficult to identify malicious emails.

51. Defendants' tactics are more effective because financial fraud victims (either as part of the compromised O365 account victim's business or their larger network) are familiar with the legitimate name of the impersonated email sender as well as the genuine domain name that the homoglyph imposter domain name impersonates, all of which make it less likely the

victim will suspect malicious activity.

52. Defendants' conduct is fraudulent and deceptive and designed to be resilient through the use of homoglyph imposter domains registered via third-party domain providers that can be ported to any infrastructure under the Defendants' control, including outside the O365 environment, impeding Microsoft's ability to protect customers and prevent further attacks once homoglyph imposter domains are ported to third-party infrastructure.

53. Defendants are aware that their conduct violates Microsoft's terms and conditions and is against the law. As a result, once detected or addressed by Microsoft through technical tools at its disposal, Defendants will often move their malicious infrastructure (and domains) outside the Microsoft ecosystem in an attempt to continue their illegal activities, or register and host domains wholly outside Microsoft's ecosystem from the outset.

Defendants Register Homoglyph Imposter Domain Names to Impersonate Domains of Legitimate Microsoft Customers

54. Defendants have registered numerous homoglyph imposter domain names (and created numerous imitation email accounts under these domains) in furtherance of their illegal activities. The following are domain names that Defendants are currently leveraging in their infrastructure, which includes .COM top-level domains (TLD) operated by Verisign as the Internet Corporation for Assigned Names and Numbers (ICANN) accredited registry within the Eastern District of Virginia.

55. Defendants registered multiple homoglyph imposter domains listed below including the one used above in soliciting a fraudulent wire transfer:

Homoglyph Imposter Domains	**Registrar**
ccp-edu.com	NameSilo, LLC
junctionfuelings.com	NameSilo, LLC
lverk.com	NameSilo, LLC

tattersails.com	NameSilo, LLC
cupidoconstructlon.com	NameSilo, LLC
thegiaint.com	NameSilo, LLC
leaseacceierator.com	NameSilo, LLC
kimballlnternational.com	NameSilo, LLC
nationalsafetyconsuiting.com	NameSilo, LLC
ldisuperstore.com	NameSilo, LLC
lithlumamericas.com	NameSilo, LLC
usgeomatlcs.com	NameSilo, LLC
ldimn.com	NameSilo, LLC
aerocerts.com	NameSilo, LLC
napieslegal.com	NameSilo, LLC
sllao.ca	KS Domains Ltd./Key Systems GmbH
exarr.co	NameSilo, LLC

56. These domain names used by Defendants are identified in **Appendix A** to the Complaint.

Defendants Attacked Many Microsoft Customers in the Eastern District of Virginia and Around the World

57. Defendants affirmatively targeted Microsoft customers in Virginia, including the Eastern District of Virginia, and throughout the United States and the world.

58. In addition, Defendants registered homoglyph imposter domains through domain registries located in the Eastern District of Virginia.

Harm to Microsoft

59. Microsoft® is a provider of the Office 365® cloud-based business and productivity suite of services. Microsoft has invested substantial resources in developing and marketing resilient and secure cloud services. Due to the security and effectiveness of Microsoft's services, Microsoft has generated substantial trust with its customers to protect their data, has established a strong brand as a leader in the security market, and has developed the Microsoft name and the names of its services into famous world-wide symbols that are well-recognized within its channels of trade.

60. Defendants have obtained login credentials stolen from Microsoft customers and unlawfully used those credentials to gain unauthorized access to Office 365 accounts in an effort to identify potential victims and opportunities to fraudulently solicit wire transfers. Defendants register homoglyph imposter domains, host those domains on fraudulently procured O365 tenants, and establish impersonation email addresses in an effort to insert themselves into legitimate business conversations and deceive recipients – either O365 customers or members of their trusted networks including those using other email accounts – into transferring funds to Defendants.

61. Once identified, Microsoft can disable access to fraudulent O365 tenants and accounts. However, even once Defendants lose access to the compromised O365 tenant, Defendants still own the homoglyph imposter domain names they registered and can move those domains to other domain registrars and hosting facilities, where they can set up new email accounts on the domains outside of Microsoft's ecosystem, and then use those domains and associated emails to continue their attacks on Microsoft, Microsoft customers and their trusted networks. Alternatively, Defendants can also register domains and host those domains from the outset through third party domain registrars and hosting facilities beyond Microsoft's control.

62. In essence, after registering the homoglyph imposter domains, Defendants have portable, weaponized mail exchange domains that can be associated to any email service provider and then used in the future to attack Microsoft customers. The threat is ongoing and pervasive, since Defendants now have the necessary tools, information, and capability to perpetrate further attacks.

63. All of these activities cause injury to Microsoft. Customers expect Microsoft to provide safe and trustworthy products and services. There is a great risk that Microsoft's

customers may incorrectly attribute Defendants' malicious activities to Microsoft's products and services. Further, Defendants' ability to damage Microsoft's reputation extends even after they are detected and lose access to O365 since they can take their weaponized domains to other platforms and continue attacks. Victims of Defendants' malicious attacks may incorrectly believe that Microsoft is the source of problems, harming customer relationships, or devaluing O365 as a platform, which further causes reputational injury to Microsoft – all because of Defendants' malicious activity and financial fraud.

64. Microsoft is similarly injured because Defendants attempt to launch their scheme from within Microsoft's Office 365 service in an effort to victimize Microsoft customers. Microsoft must bear an extraordinary burden to address cybercrime directed at its services and customers. Microsoft must develop technical countermeasures and defenses, to suppress Defendants' activities, address customer service issues caused by Defendants and must expend substantial resources dealing with the injury and confusion and to resist ongoing attempted attacks on its infrastructure, products, services, and customers. Given that Defendants continue to target Microsoft and its customers, and that such attacks will be ongoing, this poses severe risk of injury to Microsoft, threatening Microsoft's brands and customer relationships.

65. Microsoft customers may incorrectly attribute the negative impact of Defendants' activity to Microsoft. If permitted to continue unabated, there is a serious risk that Defendants may interfere with Microsoft's customer relationships.

FIRST CLAIM FOR RELIEF

Violation of the Computer Fraud & Abuse Act, 18 U.S.C. § 1030

66. Microsoft incorporates by reference each and every allegation set forth above.

67. Defendants knowingly and intentionally used login credentials stolen from

Microsoft customers to access or attempt to access protected computers and networks of Microsoft cloud services using the online accounts of Microsoft's customers without authorization and knowingly caused and/or attempted to cause the transmission of a program, information, code and commands, resulting in damage to the protected computers and networks, the software residing thereon, and Microsoft.

68. Defendants' conduct involved interstate and/or foreign communications.

69. Defendants' conduct has caused a loss to Microsoft during a one-year period aggregating at least $5,000.

70. Microsoft seeks injunctive relief and compensatory and punitive damages under 18 U.S.C. §1030(g) in an amount to be proven at trial.

71. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

SECOND CLAIM FOR RELIEF

Violation of the Stored Communications Act, 18 U.S.C. § 2701 *et seq.*

72. Microsoft incorporates by reference each and every allegation set forth above.

73. On information and belief, Doe Defendants intentionally accessed without authorization, using credentials stolen from Microsoft customers, electronic communications from protected computers and networks of Microsoft cloud services using the online accounts of Microsoft's customers.

74. On information and belief, Doe Defendants used and endeavored to use the contents of the electronic communications of Microsoft's customers, while knowing that such contents were obtained through unlawful interception.

75. Doe Defendants engaged in such actions with a knowing and/or intentional state of mind, and such actions constitute a violation of the Stored Communications Act.

76. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

77. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

THIRD CLAIM FOR RELIEF

Virginia Computer Crimes Act (Virginia Code Ann. § 18.2-152.1)

78. Microsoft incorporates by reference each and every allegation set forth above.

79. Doe Defendants, unlawfully using login credentials stolen from Microsoft customers, intentionally and maliciously used a computer and computer network to cause injury to the property of Microsoft and its customers.

80. Doe Defendants, unlawfully using login credentials stolen from Microsoft customers, intentionally and maliciously used a computer and computer network to make, or cause to be made, an unauthorized copy of computer data, residing in and communicated by Microsoft's customer's email accounts.

81. Doe Defendants, unlawfully using login credentials stolen from Microsoft customers, intentionally and maliciously used a computer and computer network to effect the creation or alteration of a financial instrument or of an electronic transfer of funds.

82. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

83. As a direct result of Defendants' actions, Microsoft has suffered and continue to

suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

FOURTH CLAIM FOR RELIEF

Common Law Trespass to Chattels

84. Microsoft incorporates by reference each and every allegation set forth above.

85. Defendants have used a computer and/or computer network, without authority, with the intent to cause physical injury to the property of another.

86. Defendants have, without authority, used a computer and/or computer network of Microsoft and the online accounts of Microsoft's customers, without authority, with the intent to trespass on the computers, computer networks, and/or online accounts of Microsoft and its customers.

87. Defendants intentionally caused this conduct and this conduct was unlawful and unauthorized.

88. Defendants' actions have caused injury to Microsoft and have interfered with the possessory interests of Microsoft over its software, services, servers, and protected computers.

89. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

90. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

FIFTH CLAIM FOR RELIEF

Conversion

91. Microsoft incorporates by reference each and every allegation set forth above.

92. Microsoft owns all right, title, and interest in its Office 365 software and services. Microsoft licenses its software to end-users. Defendants have interfered with, unlawfully and without authorization, and dispossessed Microsoft of control over its Office 365 software and services.

93. Defendants have, without authority, used a computer and/or computer network, without authority, with the intent to remove, halt, or otherwise disable or impair computer data, computer programs, and computer software from a computer or computer network.

94. Defendants have, without authority, used a computer and/or computer network, without authority, with the intent to cause a computer to malfunction.

95. Defendants have, without authority, dispossessed Microsoft of control over its computers and computer networks and have dispossessed Microsoft and its customers of control over O365 software and services.

96. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial, including without limitation the return of Defendants' ill-gotten profits.

97. As a direct result of Defendants' actions, Microsoft suffered and continue to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays that the Court:

1. Enter judgment in favor of Microsoft and against the Defendants.

2. Declare that Defendants' conduct is willful and that Defendants acted with fraud, malice and oppression.

3. Enter a preliminary and permanent injunction enjoining Defendants and their officers, directors, principals, agents, servants, employees, successors, and assigns, and all persons and entities in active concert or participation with them, from engaging in any of the activity complained of herein or from causing any of the injury complained of herein and from assisting, aiding or abetting any other person or business entity in engaging in or performing any of the activity complained of herein or from causing any of the injury complained of herein.

4. Enter a preliminary and permanent injunction directing domain registrars to disable the domains used by Defendants to cause injury and enjoining Defendants from using such domains or any other similar instrumentalities.

5. Enter judgment awarding Plaintiff actual damages from Defendants adequate to compensate Plaintiff for Defendants' activity complained of herein and for any injury complained of herein, including but not limited to interest and costs, in an amount to be proven at trial.

6. Enter judgment disgorging Defendants' profits.

7. Enter judgment awarding enhanced, exemplary and special damages, in an amount to be proved at trial.

8. Enter judgment awarding attorneys' fees and costs, and

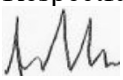
9. Order such other relief that the Court deems just and reasonable.

DEMAND FOR JURY TRIAL

Microsoft respectfully requests a trial by jury on all issues so triable in accordance with Fed. R. Civ. P. 38.

Dated: July 13, 2021

Respectfully submitted,



Julia Milewski (VA Bar No. 82426)
Matthew Welling (*pro hac vice pending*)
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington DC 20004-2595
Telephone: (202) 624-2500
Fax: (202) 628-5116
jmilewski@crowell.com
mwelling@crowell.com

Gabriel M. Ramsey (*pro hac vice pending*)
Kayvan M. Ghaffari (*pro hac vice pending*)
CROWELL & MORING LLP
3 Embarcadero Center, 26th Floor
San Francisco, CA 94111
Telephone: (415) 986-2800
Fax: (415) 986-2827
gramsey@crowell.com
kghaffari@crowell.com

Attorneys for Plaintiff Microsoft Corporation